Page 23, paragraph starting at line 28, ending at page 24, line 8:

Examples of authorized third-party execution of electronic transmissions include accessing data in third-party **28** databases or servers, processing data by third-party databases **28** or servers, presenting or displaying data to the user by a third-party database **28**, or processing of data by the DPC **10**. If the third-party is a person, the user may register a biometric with the Identicator **12**. If the third-party is an entity, such as a corporation, it may register a digital certificate with the Identicator **12**. Third-party digital certificates are available from certifying authorities, and they provide the assurance that the entity with the certificate is the authentic owner of that identity. These certificates contain readable text and other information that describes the entity. These certificates include corporate logos, a corporate address, as well as the company name.

Page 25, paragraph starting at line 10, ending at line 13:

In another embodiment where a PIC is used for identification purposes as shown in Fig. 6, a biometric theft resolution step is preferably employed, to change a user's PIC when it is determined that a user's biometric sample **62** has been fraudulently used or duplicated.

Page 25, paragraph starting at line 15, ending at line 25:

In this embodiment, a user registers with the DPC **10** as a primary user. This means that the primary user may restrict, modify, or otherwise control a subordinated user's electronic transmissions to access, process or present electronic data and electronic content stored on various third-party **28** Execution Modules **38** or third-party **28** databases. This may be desired, for example, when the primary user is a parent who wishes to influence or govern the on-line browsing activity of their minor child, who as the subordinated user is permitted access to certain desirable electronic databases while being denied access to undesirable electronic databases. In this embodiment of the invention, the primary user registers with the DPC **10** their biometric sample **62** along with the subordinated user's biometric sample **62**. Separate and unique User ID Codes are issued by the Identicator for the primary user and the subordinated user, respectively.

Page 32, paragraph starting at line 15, ending at line 21:

The Clearinghouse **14** optionally stores user-customized Pattern Data **54** that is unassociated with any user-customized Execution Commands 52 and optionally stores user-customized Execution Commands **52** that are not associated with any user-customized Pattern Data **54**. Therefore, such unassociated Pattern Data **54** or Execution Commands **52** are optionally stored within the Clearinghouse **14** until they are associated with a Pattern Data **54** or an Execution Command **52** together thereby forming an executable Rule Module.

Page 36, paragraphs starting at line 13, ending at page 37, line 15:

Upon the Identicator's successful identification of the user from their bid biometric, other embodiments of Execution Commands **52** governing electronic transmission access include permitting the user to access their health insurance account and validate their benefits to a health-care provider prior to being admitted to a hospital, to access their pre-paid entertainment account and validate to admittance personnel their eligibility to attend an entertainment event, such as a live music concert on a pre-prescribed day, at a pre-prescribed time and to sit in a pre-prescribed seat, to access their video club account and validate to a merchant their eligibility to rent videos under their pre-paid membership, to access their driver's license on-line and validate to an authority their eligibility to drive a car, to purchase restricted products like alcohol or tobacco, or to access a restricted entertainment event such as an R-rated film being shown in theatres, to access their credit-rating account and validate to a cashier their eligibility for check-writing privileges, to access an Internet web site and enter a real-time chat room with other people on-line.

Further embodiments of Execution Commands **52** governing electronic transmission access include entitling a user to extend an on-line user-customized session by repeating their user-customized session log-in by entering either their biometric or at least one of their user-customized Pattern Data **54** when periodically queried to do so by the Identicator **12** or Clearinghouse **14**, to access customized radio or television programming, wherein the user can be provided with customized programming, with or without time restrictions, that reflects pre-designated preferences, such as a channel broadcasting only news on companies in which the user has an investment or a channel broadcasting only music from Broadway theater shows which the user has seen or

indicated a desire to see, to access restricted portions of corporate intranet 58 databases on a selective basis, based upon pre-designated Pattern Data 54, such as the user's job title or company division, to access their travel reservations and validate to the admittance attendant that the user is eligible to travel, such as boarding a particular flight or a specific train, on a pre-prescribed day, at a pre-prescribed time, and to sit in a pre-prescribed seat, to access on-line position "papers" of user-customized political candidates and electoral ballot initiatives, and validate to an authorized third-party that the user is eligible to vote in particular elections, such as voting for a particular candidate running from a particular user-customized district.

Page 38, paragraph starting at line 19, ending at line 28:

As an example of the above, the user's intelligent agent can direct the user's search engine to automatically conduct periodic, customized on-line data retrievals reflecting user-customized priorities for: product or service promotional offers or discounts via email or instant messaging; user-customized investment updates; user-customized medical or health information; competitive product or service prices across a broad range of on-line merchants; hobby or recreational interests; interactive user-customized on-line advertisements, wherein product or service providers are permitted to provide unsolicited information to a user based upon certain user-customized criteria; on-line event calendaring, wherein a user is automatically notified of upcoming events or activities reflecting their interests.

Page 39, paragraph starting at line 24, ending at page 40, line 9:

In another embodiment where greater security is required, an Execution Command **52** governs the appending of a user-unique network credential or digital certificate to an electronic transmission. If a user employing a biometric seeks to append their digital certificate to an electronic transmission, the user stores at least one command to sign electronic documents using their private keys, which are themselves centrally stored on a Clearinghouse **14** server. As such, the user's private keys are invoked as a header for the user's electronic transmission which, in combination with the electronic document itself and an MD5 calculation of the document, together form a digital signature. At a later time, an authorized recipient can use the user's public key from the DPC **10** or a third-party certifier to verify the authenticity of the sender and the electronic

document's contents to yield a secure, authenticated electronic transmission. In this way, users do not have to manage their own private keys, nor do they have to retain physical possession of their digital certificates via smart cards or personal computers with resident user-customized data. In one embodiment, public keys of a particular certifying authority are initially stored in the BIA **16** at the time of construction.

Page 43, paragraph starting at line 21, ending at line 28:

The DPC **10** forwards to the BIA **16** a unique, one-time usage Random Key Number (RKN), optionally one for each and every one of said third-party database **28** Internet locations which are relevant to the user. The BIA **16** will store the Random Key Number in Random Access Memory (RAM), and will erase them when the user's log-on session terminates. These Random Key Numbers are preferably sent from the DPC **10** to the BIA **16** as encrypted 128-bit random number. The BIA **16** decrypts the Random Key Number and forwards it to the kiosk. At this point, the kiosk is permitted to display or present all such URLs for the user as text or- preferably as visual icons.

Page 45, paragraph starting at line 8, ending at line 24:

Further, in this embodiment, the user on the "Messaging" icon to access all of their email, Internet fax and Internet voicemail messaging accounts. The "Messaging" icon, represents all of the URLs related to the user's messaging accounts which have been grouped by the Clearinghouse **14** according to the user's Rule Modules **50** . The user has previously stored with [theClearinghouse] the Clearinghouse **14** their messaging account URLs along with their respective account names and passwords. Once the user clicks on the kiosk's "get new messages" icon, the kiosk requests the DPC **10** to access the user's messaging accounts. Once this request is received by the DPC, the Clearinghouse **14** invokes the user's Rule Modules **50** governing message requests. Assuming the user wants to simultaneously obtain all of their messages at once, the DPC **10** in turn sends a HyperText Transfer Protocol (HTTP) "get" message command for each URL, thereby enabling the DPC **10** to retrieve all of their email, Internet voicemail and Internet fax account messages at once. (Note that HTTP is the protocol currently used to transfer information from Internet third-party databases **28** to client browsers.) These messages are the Pull Data retrieved by the DPC. The DPC **10** filters

the HyperText Markup Language (HTML) to retain only user-relevant message contents and forward this to the kiosk for presentation to the user.

Page 46, paragraph starting at line 3, ending at line 18:

In this embodiment, one of the user's invoked Rule Modules **50** that provide calendaring functions, the kiosk automatically presents the user with an "Academics" icon for notification that they must complete their university's on-line coursework examination. In this embodiment, the DPC **10** provides the BIA **16** with a packet containing the Universal Access Command, the Random Key Number, and any other relevant user-unique network credentials for the university's restricted database. The BIA **16** decrypts this packet and forwards it to the kiosk for display to the user. The user clicks on the displayed icon representing the URL for the third-party Execution Module 38 and databases at which resides the examination for which the user has pre-registered. The kiosk forwards Random Key Number to the URL, and the resident Execution Module **38** queries the DPC **10** to authenticate the validity of the Random Key Number. If the DPC **10** confirms the validity of the Random Key Number to the URL, the user is enabled to access the third party database and take their electronically stored course exam. Preferably for security, this particular Random Key Number would be good for only one on-line session by the user with the relevant third-party database, in this case being the university server on which is stored the course examination.

Page 50, paragraph starting at line 14 and ending at line 29:

In one embodiment, the Identicator **12** module is physically distinct and separate from the Clearinghouse **14** module with each housed in independent servers or modules. In another embodiment, the Identicator is physically integrated with the Clearinghouse, whereby the Identicator **12** and Clearinghouse **14** are physically interconnected and integrated together within one server or module. In both embodiments, communications between the Identicator and the Clearinghouse **14** occur via many different methods and means that are well known in the art. Most depend on the particular communication networks already deployed by the organization or company that deploys the electronic transmission authorization system.

In one embodiment the, the Identicator and the Clearinghouse **14** are connected via Ethernet to a local router, which is connected to a network operations center (NOC) via frame relay lines. Messages are sent between the Identicator and the Clearinghouse **14** using TCP/IP over this network. In another embodiment, the Identicator and the Clearinghouse **14** are connected via a cellular digital packet data (CDPD) modem to a CDPD provider, who provides TCP/IP connectivity from the Identicator to an intranet **58** to which at least one Clearinghouse **14** is attached.

Page 51, paragraph starting at line 1, ending at line 6:

In yet another embodiment, an Identicator is connected via the Internet, as is at least one Clearinghouse. TCP/IP is used to transmit messages from between the Identicator and the Clearinghouse. There are many different ways to connect the Identicator and the Clearinghouse **14** that are well understood in the industry, such as cable TV networks, cellular telephone networks, telephone networks, the Internet, an intranet, a LAN, a WAN, or an X.25 network.

Page 51, paragraph starting at line 9, ending at line 14:

The Identicator and the Clearinghouse **14** hardware modules are high-reliability database servers, well known in the art, such as those available from Sun™, Compaq™, Tandem™, IBM™ and the like. Further, the Identicator and the Clearinghouse **14** software may incorporate scalable database architecture, well known in the art, such as those available from Oracle™, Sybase™, Informix™ and the like.

Page 51, paragraph starting at line 18, ending at page 52, line 2:

In certain embodiments, a master Identicator is responsible for storage of the entire set of biometric samples and digital certificates registered for use with this invention. The master Clearinghouse **14** is responsible for storage of the entire set of Pattern Data **54**, Execution Commands **52**, and Rule Modules **50** registered for use with this invention.

Each master Identicator and master Clearinghouse **14** site is preferably made up of a number of computers and databases connected together over a LAN (known in the industry).

Multiple and redundant master computer sites ensure reliable service in the face of disaster or serious hardware failure at any single central computer site.

Local Identicator servers store subsets of the entire set of biometric samples and digital certificates registered for use with this invention. Local Clearinghouse **14** servers store subsets of the entire set of Pattern Data 54, Execution Commands 52, and Rule Modules **50** registered for use with this invention. Such Pattern Data **54** and Execution Commands **52** subsets are circumscribed by any number of criteria including, usage location, usage frequency, usage recency, usage demographics and usage volume of electronic transmissions.

Page 52, paragraphs starting at line 13, ending at page 53, line 7:

This system comprises at least one master Identicator and one master Clearinghouse, which contains a large subset of all parties registered with the system. The system further comprises at least two local Identicators or two local Clearinghouses that are physically apart from each other. Each local Identicator or Clearinghouse **14** contains a subset of the parties contained within the master Identicator or Clearinghouse. Data communications lines allow electronic transmissions to flow between each local Identicator or Clearinghouse **14** and the master Identicator or Clearinghouse.

In this embodiment, identification request electronic transmissions are first sent to the local Identicator or Clearinghouse **14** for processing. If a party cannot be identified by the local Identicator or if the requisite Rule Module is not contained in the local Clearinghouse, the electronic transmission is forwarded to the master Identicator or Clearinghouse. If the parties are identified properly by the master Identicator or if the requisite Rule Module is located in the master Clearinghouse, the electronic transmission is processed appropriately. In addition, the user's identity information can be transmitted from the master Identicator to the local Identicator, so that the next time the user will be successfully identified by the local Identicator.

In another embodiment of a use-sensitive system, the system further comprises a purge engine for deleting a party's user-customized information from the local Identicator and Clearinghouse **14** databases. In order to store only records for those parties who use the system more than a prescribed frequency and prevent the overload of databases with records from parties who use the system only occasionally, the record of a party is deleted from the

local Identicator and Clearinghouse **14** databases if there has been no attempt to identify the party upon expiration of a predetermined time limit.

Page 53, paragraph starting at line 14, ending at line 19:

In one embodiment, an Execution Command **52** optionally requires the Clearinghouse **14** and the Execution Module **38** to communicate with at least one third-party **28** computer or database to conduct the user's command. For example, when the Execution Module **38** communicates with a host server located within an educational institution, where the third-party database **28** stores research data which is accessed in order to complete the user's Execution Command **52**.

Page 54, paragraph starting at line 24, ending at line 26:

The firewall **40** provides a first line of defense against network viruses and computer hackers. All communication links into or out of the Identicator **12** and Clearinghouse **14** server sites first pass through a secure firewall **40** Machine.

Page 55, paragraphs starting at line 1, ending at line 8:

BIA–equipped terminals send packets to Identicator **12** and Clearinghouse **14** server sites via modem, X.25, or other communication medium. The Identicator **12** and Clearinghouse **14** server sites rely on a third-party to supply the modem banks required to handle the volume of calls and feed the data onto the DPC **10** backbone.

For communications between Identicator **12** and Clearinghouse **14** server sites, the FW Machines send out double–length DES encrypted packets. The server site LAN component handles the encryption and decryption: the firewall **40** does not have the ability to decrypt the packets.